



SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

03 listopada 2026 r.

Typ 200

Monitorowanie i wykrywanie incydentów w IT/OT

Esecure sp. z o.o.

10:00 – 10:05 **Zasady organizacyjne przebiegu szkolenia**

Przedstawiciel Departamentu Cyberbezpieczeństwa MC

10:05 – 12:00 **SIEM w pigułce – fundamenty nowoczesnego cyberbezpieczeństwa**

- poznaj SecureVisio – jedna platforma, wiele możliwości
- architektura rozwiązania – co kryje się pod maską?
- od źródła do systemu – metody pozyskiwania logów
- świat OT – specyfika środowisk przemysłowych
- IT vs OT – dwa światy, różne wyzwania
- parsowanie logów – od surowych danych do wartościowych informacji
- panel parserów – konfiguracja i zarządzanie w praktyce
- przeglądarka logów – analiza i wyszukiwanie zdarzeń
- reguły bezpieczeństwa – jak wykrywać zagrożenia?
- od zdarzenia do incydentu – analiza i obsługa incydentów
- asystent AI – sztuczna inteligencja w służbie analityka SOC
- UEBA – wykrywanie anomalii i nietypowych zachowań
- wizualizacja danych – logi przedstawione w czytelnej formie

Ekspert Esecure: Krzysztof INGLÓT

12:00 – 12:10 **Sesja pytań i odpowiedzi.**
